**MOP to deploy SSL Certificate with SAN of Kafka broker**

Owned by [Vishnu Gupta](https://clairvoyant.atlassian.net/wiki/people/628e0878c65b72006961f46d?ref=confluence&src=profilecard)

Nov 30, 2023

2 min read

13 people viewed

After you receive the signed cert, please follow the steps specified below to deploy the certs into the KeyStore of the given broker

**Pre-Deployment Validation Steps**

**Step 1**: - Stop the Broker from cloudera manager and put it under maintenance

**Step 2**: - validate the new signed cert against the existing CA file available on the broker host

]$ openssl verify -CAfile /opt/cloudera/security/CAcerts/ca.cert.pem kprd20.pem

Above command should return "**OK**"

**Step 3**: - Open the provided cert and scan the expiry date, Issuers name, Subject name, EKU should have TLS WebClient and TLS Webserver both and finally should have a SAN name same as the CN name, which should be the host FQDN

]$ openssl x509 -in kprd20.pem -noout -text

After you have done examining the new cert, Let’s move ahead with the Deployment steps

**Deployment Steps**

**Step 4**: - Create a KeyStore in PKcs12 format and import the private key that was generated at the time of CSR generation into the new KeyStore. I have already copied the private keys for each broker cert in my home directory of that broker

] $openssl pkcs12 -export -inkey /home/vgupta/kprd20.key -in kprd20.pem -out kprd20.p12

**Step 5**: - Convert the PKCS12 KeyStore into JKS format

keytool -importkeystore -srckeystore kprd20.p12 -srcstorepass <KS-PASSWD> -srckeypass <KS-PASSWD> -destkeystore kprd20.jks -deststoretype JKS -srcalias 1 -deststorepass <KS-PASSWD> -destkeypass <KS-PASSWD>

**Step 6**: - Import the Intermediate CA into the new JKS KeyStore,

]$ keytool -importcert -alias subordinateca -file /home/vgupta/ca-chain.cert.pem -KeyStore kprd20.jks

**Step 7**: - Import the root CA into the new KeyStore

] $keytool -importcert -alias rootca -file /opt/cloudera/security/CAcerts/ca.cert.pem -keystore kprd20.jks

**Step 8**: - validate the new keystore to ensure that it has the new leaf cert with the DNS name as the host FQDN, the intermediate CA with the alias "subordinateca" and a Root CA with the alias "rootca"

]$ keytool -v -list -keystore kprd20.jks

**Step 9**: - Replace the Old Keystore with the New

] $mv /opt/cloudera/security/jks/kafka-keystore.jks /opt/cloudera/security/jks/kafka-keystore-oldbkp.jks

] $cp kprd20.jks /opt/cloudera/security/jks/kafka-keystore.jks

**Step 10**: - Restart the Broker from Cloudera Manager

**Step 11**: - Post Deployment Validation Step

] $openssl s\_client -connect <Broker FQDN>:9093 </dev/null 2>/dev/null |openssl x509 -noout -text |grep -A 1 "Subject Alternative Name"

X509v3 Subject Alternative Name:

DNS:<Broker-FQDN>

After successful validation, please take the broker out of maintenance and ask the Application to run validations at their end